A B S T R A C T

A METHOD OF MAKING SECURE THE TRANSMISSION OF A MESSAGE FROM AN EMITTER DEVICE TO A RECEIVER DEVICE

The invention relates to a method of making secure the transmission of a message (Prgm) from an emitter device (E) to a receiver device (R). The method of the invention is characterized in that: the message (Prgm) is subdivided into n elementary units (I), where n is a number greater than or equal to 1; a logical property (P) is defined in such a manner that for any elementary unit (I), the logical property (P) applied to an authentic elementary unit (I) gives a logical value of the type true; the message (Prgm) is encrypted by encryption means of the emitter device (E) using an encryption algorithm having a key (Kc) so as to obtain a result Kc(Prgm); the encrypted result Kc(Prgm) is transmitted by the emitter device (E) to the receiver device (R); the encrypted result Kc(Prgm) is decrypted by the receiver device (R) using a decryption algorithm having a secret key (Kd) so as to obtain a decrypted result Kd(Kc(Prgm)); the decrypted result Kd(Kc(Prgm)) is subdivided into elementary units (I); the logical property (P) is applied to the elementary units (I) so as to obtain, for each unit, a logical value of the type true or of the type false. The invention is particularly applicable to the field of smart cards.

Translation of the title and the abstract as they were when originally filed by the Applicant. No account has been taken of any changes that may have been made subsequently by the PCT Authorities acting ex officio, e.g. under PCT Rules 37.2, 38.2, and/or 48.3.